Software Improvement Group

OPENBARE SAMENVATTING

SBIR CYBER SECURITY

Cyber Security: door toeval of door design?

Uitgevoerd door de Software Improvement Group in samenwerking met de Radboud Universiteit Nijmegen.

In het kader van de Nationale Cyber Security Research Agenda heeft Rijksdienst voor Ondernemend Nederland (RVO) de opdracht verstrekt aan de Software Improvement Group (SIG) om haar toetsingsmethode voor de ingebouwde veiligheid van softwaresystemen door te ontwikkelen. De methode is inmiddels succesvol toegepast op ruim 30 software-systemen van overheden, telecombedrijven en financiële instellingen.

Cyber Security – door toeval?

Veel organisaties gebruiken firewalls en voeren regelmatig securitytesten uit. Desondanks neemt het aantal security-incidenten sterk toe. Blijkbaar is er nog geen grip op informatiebeveiliging. De weerbaarheid van de diensten waarvan we allemaal afhankelijk zijn is daardoor in het geding, evenals de vertrouwelijkheid van onze gegevens.

Er ligt een enorme kans om deze grip te verbeteren. Onderzoek toont namelijk aan dat 75% van de security-incidenten wordt veroorzaakt door fouten tijdens het bouwen van software. Daaraan wordt nog relatief weinig aandacht besteed omdat het zo moeilijk is de security van software te doorgronden. Fouten komen vaak pas aan het licht als de software klaar is, tijdens een test, of erger nog; door een incident. Een dergelijke (penetratie)test probeert een aantal bekende vormen van misbruik, maar kan niet beoordelen of security goed is ingebouwd.

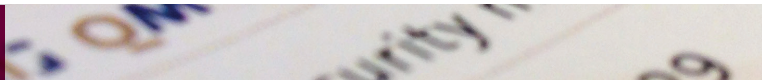
SIG heeft een methode ontwikkeld om de kwaliteit van security in software te bepalen, tijdens en na het ontwikkelen. Systematische analyse van de broncode en het daarin vervatte ontwerp staan centraal in de methode, gebruik makend van een slimme mix van tooling en handmatige review. Daarnaast worden resultaten van securitytesten betrokken en analyseert de methode de context om zwakheden te vinden, risico's en daarmee prioriteiten te bepalen en te adviseren over verbetering: in het ontwikkelproces, technologiekeuze en configuratie.

De methode omvat het op ISO 25010 gebaseerde securitymodel, een analyse-aanpak, tooling, opleiding voor consultants en een kennisbank van software security best practices.

'Getting software security right'

SIG heeft in samenwerking met Radboud Universiteit Nijmegen in 2013 en 2014 de SIG Quality Model (SIG QM) securitymethode doorontwikkeld en getoetst. Voor dit project heeft RVO vanuit SBIR subsidie verleend. SIG heeft daarnaast ook zelf fors geïnvesteerd in onderzoek en ontwikkeling.

Software Improvement Group



De methode is tot stand gekomen door middel van wetenschappelijk onderzoek, interviews en door ervaring tijdens ruim 30 projecten waarin de methode is toegepast. Deze projecten zijn uitgevoerd op uiteenlopende systemen in verschillende sectoren en deze hebben de herhaalbaarheid, objectiviteit, efficiëntie en effectiviteit geoptimaliseerd.

Gebaseerd op de resultaten van het onderzoek trekt SIG de volgende conclusies:

- Het securitymodel en de analyse-aanpak hebben een aantoonbare meerwaarde voor software security.
- De methode is economisch rendabel en draagt bij aan versterking van de Nederlandse Cyber Security economie.
- De aanpak draagt bij aan een betere voorbereiding op toekomstige security uitdagingen door ‘security by design’.
- De methode leent zich goed voor risicomanagement en kan daardoor ingezet worden voor aansturing van ICT-projecten en portfolio’s.

Cyber Security – door design!

SIG is erin geslaagd om bestaande kennisbronnen en standaarden te bundelen om herhaalbaar, systematisch, consistent en meetbaar te beoordelen of software veilig is gebouwd en daarover te adviseren. Door security inzichtelijk te maken wordt het geen toeval meer, maar ‘security by design’, bij voorkeur vanaf het begin van de ontwikkeling.

Gebaseerd op het onderzoek en de opgedane contacten in het vakgebied, verwacht SIG een grotere bewustwording. Bewustwording dat software een steeds grotere rol speelt, bewustwording van het belang van security en bewustwording van op welke manier je daarvoor zorgt draagt.

Samenwerking voor innovatie

Door de ondersteuning van SBIR heeft SIG het securitymodel sneller en met meer diepgang kunnen ontwikkelen en op de markt kunnen brengen. Dat stelt SIG in staat om rasse schreden te maken op het gebied van cyber security in software.

SIG houdt zich actief bezig met onderzoek en innovatie op het gebied van software-metrieken, kwaliteitsstandaarden, softwarestructuren en testtechnieken. In dit onderzoek is samengewerkt met de onderzoeksgroep Digital Security van de Radboud Universiteit Nijmegen. De onderzoeksgroep Digital Security heeft SIG in dit project aangevuld met kennis en expertise op het gebied van security assessment, verificatie en secure software-engineering.

Contact

Voor meer informatie kunt u contact opnemen met:
Rob van der Veer
Principal Consultant Security
06 20 43 71 87
r.vanderveer@sig.eu

Software Improvement Group
Amstelplein 1, 1096 HA Amsterdam
www.sig.eu

Dit onderzoek is tot stand gekomen in samenwerking met:

Radboud Universiteit Nijmegen